What is claimed is:

1. A method for generating prime numbers, the method comprising the steps of:

   a. generating a random number ‘n’;

   b. checking if the random number ‘n’ is an exact power of another positive integer;

   if the random number ‘n’ is an exact power of another positive integer, then:

   c. declaring the random number ‘n’ to be composite; and

   if the random number ‘n’ is not an exact power of another positive integer, then:

   d. performing an extension ring test on the random number ‘n’.

2. The method as recited in claim 1 wherein the step of performing the extension ring test comprises the steps of:

   a. choosing a set of polynomials g(x);

   b. choosing a polynomial f(x);

   if $[g(x)]^n \neq g(x^n)$ mod(f(x), n), for the chosen f(x) and any g(x) belonging to the chosen set of polynomials g(x) then:

   c. declaring the random number ‘n’ to be composite; and

   if $[g(x)]^n = g(x^n)$ mod(f(x), n), for the chosen f(x) and all g(x) belonging to the chosen set of polynomials g(x) then:

   d. declaring the random number ‘n’ to be prime.

3. The method as recited in claim 1 wherein the step of performing the extension ring test comprises the steps of:

   a. determining the smallest number ‘r’ less than the random number ‘n’, the number ‘r’ satisfying the following conditions:

      i. the number ‘r’ is a prime number;

ii. the largest prime factor 'q' of $(r - 1)$ is greater than or equal to $(4\sqrt{r} \log_2 n)$;

iii. $n^{(r-1)/q} \neq 1 \bmod (r)$; and

iv. the greatest common divisor of the number 'r' and the random number 'n' is equal to 1;

if no number 'r' satisfying all the conditions specified in step a exists, then for all values of the number 'r' less than the random number 'n':

b. performing a check whether the greatest common divisor of the number 'r' and the random number 'n' is greater than 1;

if the greatest common divisor of 'r' and 'n' is greater than 1 for any value of the number 'r', then:

i. declaring the number 'n' to be composite;

if the greatest common divisor of 'r' and 'n' is equal to 1 for all values of the number 'r', then:

ii. declaring the number 'n' to be prime; and

if a number 'r' satisfying the conditions specified in step a exists, then:

c. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and $(2\sqrt{r} \log_2 n)$, then:

i. declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$, then:

ii. declaring the random number 'n' to be prime.

4. A method for generating prime numbers, the method comprising the steps of:

   a. generating a random number 'n';

   b. checking if the random number 'n' is an exact power of another positive integer;

   if the random number 'n' is an exact power of another positive integer, then:

   c. declaring the random number 'n' to be composite; and

   if the random number 'n' is not an exact power of another positive integer, then:

   d. performing an extension ring test, the extension ring test comprising:

      i. determining the smallest number 'r' less than the random number 'n', the number 'r' satisfying the following conditions:

         1. the number 'r' is a prime number;

         2. the largest prime factor 'q' of $(r - 1)$ is greater than or equal to $(4\sqrt{r} \log_2 n)$;

         3. $n^{(r-1)/q} \neq 1 \bmod (r)$; and

         4. the greatest common divisor of the number 'r' and the random number 'n' is equal to 1;

      if no number 'r' satisfying all the conditions specified in step a exists, then for all values of the number 'r' less than the random number 'n':

      ii. performing a check whether the greatest common divisor of the number 'r' and the random number 'n' is greater than 1; and

         if the greatest common divisor of 'r' and 'n' is greater than 1 for any value of the number 'r', then:

1. declaring the number ‘n’ to be composite; and

if the greatest common divisor of ‘r’ and ‘n’ is equal to 1 for all values of the number ‘r’, then:

2. declaring the number ‘n’ to be prime;

if a number ‘r’ satisfying the conditions specified in step a exists, then:

iii. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of ‘a’ from 1 to $(2\sqrt{r} \log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of ‘a’ between 1 and $(2\sqrt{r} \log_2 n)$, then:

1. declaring the number ‘n’ to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of ‘a’ from 1 to $(2\sqrt{r} \log_2 n)$, then:

2. declaring the random number ‘n’ to be prime.

5. The method as recited in claim 1 wherein the method is implemented as a computer program product.

6. The method as recited in claim 4 wherein the method is implemented as a computer program product.

7. A method of deterministically testing primality of a random number ‘n’ in polynomial time, the method comprising the steps of:

a. checking if the random number ‘n’ is an exact power of another positive integer;

if the random number ‘n’ is an exact power of another positive integer, then:

b. declaring the random number ‘n’ to be composite; and if the random number ‘n’ is not an exact power of another positive integer, then:

c. performing an extension ring test.

8. The method as recited in claim 7 wherein the step of performing the extension ring test comprises the steps of:

a. choosing a set of polynomials g(x);

b. choosing a polynomial f(x);

if $[g(x)]^n \neq g(x^n)$ mod(f(x), n), for the chosen f(x) and any g(x) belonging to the chosen set of polynomials g(x) then:

c. declaring the random number ‘n’ to be composite; and

if $[g(x)]^n = g(x^n)$ mod(f(x), n), for the chosen f(x) and all g(x) belonging to the chosen set of polynomials g(x) then:

d. declaring the random number ‘n’ to be prime.

9. The method as recited in claim 7 wherein the step of performing the extension ring test comprises the steps of:

a. determining the smallest number ‘r’ less than the random number ‘n’, the number ‘r’ satisfying the following conditions:

i. the number ‘r’ is a prime number;

ii. the largest prime factor ‘q’ of (r – 1) is greater than or equal to ($4\sqrt{r}$ $\log_2 n$);

iii. $n^{(r-1)/q} \neq 1$ mod (r); and

iv. the greatest common divisor of the number ‘r’ and the random number ‘n’ is equal to 1;

if no number ‘r’ satisfying all the conditions specified in step a exists, then for all values of the number ‘r’ less than the random number ‘n’:

b. performing a check whether the greatest common divisor of the number ‘r’ and the random number ‘n’ is greater than 1; and

if the greatest common divisor of ‘r’ and ‘n’ is greater than 1 for any value of the number ‘r’, then:

i. declaring the number ‘n’ to be composite; and

if the greatest common divisor of ‘r’ and ‘n’ is equal to 1 for all values of the number ‘r’, then:

ii. declaring the number ‘n’ to be prime;

if a number ‘r’ satisfying the conditions specified in step a exists, then:

c. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of ‘a’ from 1 to $(2\sqrt{r} \log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of ‘a’ between 1 and $(2\sqrt{r} \log_2 n)$, then:

i. declaring the number ‘n’ to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of ‘a’ from 1 to $(2\sqrt{r} \log_2 n)$, then:

ii. declaring the random number ‘n’ to be prime.

10. A method of deterministically testing primality of a random number ‘n’ in polynomial time, the method comprising the steps of:

a. checking if the random number ‘n’ is an exact power of another positive integer;

if the random number ‘n’ is an exact power of another positive integer, then:

b. declaring the random number ‘n’ to be composite;

if the random number ‘n’ is not an exact power of another positive integer, then:

c. performing an extension ring test, the extension ring test comprising:

   i. determining the smallest number ‘r’ less than the random number ‘n’, the number ‘r’ satisfying the following conditions:

      1. the number ‘r’ is a prime number;

      2. the largest prime factor ‘q’ of (r – 1) is greater than or equal to $(4\sqrt{r} \log_2 n)$;

      3. $n^{(r-1)/q} \neq 1 \bmod (r)$; and

      4. the greatest common divisor of the number ‘r’ and the random number ‘n’ is equal to 1;

   if no number ‘r’ satisfying all the conditions specified in step a exists, then for all values of the number ‘r’ less than the random number ‘n’:

   ii. performing a check whether the greatest common divisor of the number ‘r’ and the random number ‘n’ is greater than 1; and

      if the greatest common divisor of ‘r’ and ‘n’ is greater than 1 for any value of the number ‘r’, then:

      1. declaring the number ‘n’ to be composite; and

      if the greatest common divisor of ‘r’ and ‘n’ is equal to 1 for all values of the number ‘r’, then:

      2. declaring the number ‘n’ to be prime;

   if a number ‘r’ satisfying the conditions specified in step a exists, then:

iii. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and $(2\sqrt{r} \log_2 n)$, then:

1. declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$, then:

2. declaring the random number 'n' to be prime.

11. The method as recited in claim 7 wherein the method is implemented as a computer program product.

12. The method as recited in claim 10 wherein the method is implemented as a computer program product.

13. A system for deterministically testing primality of a random number 'n' in polynomial time, the system comprising:

a. means for checking if the random number 'n' is an exact power of another positive integer;

if the random number 'n' is an exact power of another positive integer, then:

b. means for declaring the random number 'n' to be composite; and

if the random number 'n' is not an exact power of another positive integer, and;

c. means for performing an extension ring test.

14. The system as claimed in claim 13, wherein the extension ring test comprises means for:

a. choosing a set of polynomials g(x);

b. choosing a polynomial f(x);

if $[g(x)]^n \neq g(x^n)$ mod(f(x), n), for the chosen f(x) and any g(x) belonging to the chosen set of polynomials g(x) then:

c. declaring the random number 'n' to be composite; and

if $[g(x)]^n = g(x^n)$ mod(f(x), n), for the chosen f(x) and all g(x) belonging to the chosen set of polynomials g(x) then:

d. declaring the random number 'n' to be prime.

15. The system as claimed in claim 13, wherein the extension ring test comprises means for:

a. generating a random number 'n';

b. checking if the random number 'n' is an exact power of another positive integer;

if the random number 'n' is an exact power of another positive integer, then:

c. declaring the random number 'n' to be composite; and

if the random number 'n' is not an exact power of another positive integer, then:

d. performing an extension ring test, the extension ring test comprising means for:

i. determining the smallest number 'r' less than the random number 'n', the number 'r' satisfying the following conditions:

1. the number 'r' is a prime number;

2. the largest prime factor 'q' of (r – 1) is greater than or equal to $(4\sqrt{r} \log_2 n)$;

3. $n^{(r-1)/q} \neq 1 \bmod (r)$; and

4. the greatest common divisor of the number ‘r’ and the random number ‘n’ is equal to 1;

if no number ‘r’ satisfying all the conditions specified in step a exists, then for all values of the number ‘r’ less than the random number ‘n’:

ii. performing a check whether the greatest common divisor of the number ‘r’ and the random number ‘n’ is greater than 1; and

if the greatest common divisor of ‘r’ and ‘n’ is greater than 1 for any value of the number ‘r’, then:

1. means for declaring the number ‘n’ to be composite; and

if the greatest common divisor of ‘r’ and ‘n’ is equal to 1 for all values of the number ‘r’, then:

2. means for declaring the number ‘n’ to be prime;

if a number ‘r’ satisfying the conditions specified in step a exists, then:

iii. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of ‘a’ from 1 to $(2\sqrt{r} \log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of ‘a’ between 1 and $(2\sqrt{r} \log_2 n)$, then:

1. means for declaring the number ‘n’ to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of ‘a’ from 1 to $(2\sqrt{r} \log_2 n)$, then:

2. means for declaring the random number ‘n’ to be prime.

16. A system for encrypting a communication, said system including a prime number generator, wherein the improvement comprises: the prime number generator

having a random number generator for generating a random number ‘n’ and: means for checking if the random number ‘n’ is an exact power of another positive integer; if the random number ‘n’ is an exact power of another positive integer, then declaring the random number ‘n’ to be composite; if the random number ‘n’ is not an exact power of another positive integer, then performing an extension ring test on the random number ‘n’ so as to determine whether the random number is prime.

17. The encryption system as claimed in claim 16, wherein the extension ring test comprises means for:

a. choosing a set of polynomials g(x);

b. choosing a polynomial f(x);

if $[g(x)]^n \neq g(x^n)$ mod(f(x), n), for the chosen f(x) and any g(x) belonging to the chosen set of polynomials g(x) then:

c. declaring the random number ‘n’ to be composite; and

if $[g(x)]^n = g(x^n)$ mod(f(x), n), for the chosen f(x) and all g(x) belonging to the chosen set of polynomials g(x) then:

d. declaring the random number ‘n’ to be prime.

18. The encryption system as claimed in claim 16, wherein the extension ring test comprises means for:

a. generating a random number ‘n’;

b. checking if the random number ‘n’ is an exact power of another positive integer;

if the random number ‘n’ is an exact power of another positive integer, then:

c. declaring the random number ‘n’ to be composite; and

if the random number ‘n’ is not an exact power of another positive integer, then:

d. performing an extension ring test, the extension ring test comprising means for:

   i. determining the smallest number ‘r’ less than the random number ‘n’, the number ‘r’ satisfying the following conditions:

      1. the number ‘r’ is a prime number;

      2. the largest prime factor ‘q’ of (r – 1) is greater than or equal to ($4\sqrt{r}\log_2 n$);

      3. $n^{(r-1)/q} \neq 1 \bmod (r)$; and

      4. the greatest common divisor of the number ‘r’ and the random number ‘n’ is equal to 1;

   if no number ‘r’ satisfying all the conditions specified in step a exists, then for all values of the number ‘r’ less than the random number ‘n’:

   ii. performing a check whether the greatest common divisor of the number ‘r’ and the random number ‘n’ is greater than 1; and

      if the greatest common divisor of ‘r’ and ‘n’ is greater than 1 for any value of the number ‘r’, then:

      1. means for declaring the number ‘n’ to be composite; and

      if the greatest common divisor of ‘r’ and ‘n’ is equal to 1 for all values of the number ‘r’, then:

      2. means for declaring the number ‘n’ to be prime;

   if a number ‘r’ satisfying the conditions specified in step a exists, then:

iii. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and $(2\sqrt{r} \log_2 n)$, then:

1. means for declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$, then:

2. means for declaring the random number 'n' to be prime.

19. A system for encrypting a communication, said system including a prime number generator, wherein the improvement comprises:

a. the prime number generator including:

i. a random number generator for generating a random number 'n' and:

ii. means for checking if the random number 'n' is an exact power of another positive integer;

iii. means for declaring the random number 'n' to be composite;

iv. means for performing an extension ring test on the random number 'n'; and

v. means for declaring the random number 'n' to be prime.

20. The encryption system as claimed in claim 19, wherein the means for performing the extension ring test comprise means for:

a. choosing a set of polynomials g(x);

b. choosing a polynomial f(x);

if $[g(x)]^n \neq g(x^n)$ mod(f(x), n), for the chosen f(x) and any g(x) belonging to the chosen set of polynomials g(x) then:

c. declaring the random number 'n' to be composite; and

if $[g(x)]^n = g(x^n)$ mod(f(x), n), for the chosen f(x) and all g(x) belonging to the chosen set of polynomials g(x) then:

d. declaring the random number 'n' to be prime.

21. The encryption system as claimed in claim 19, wherein the means for performing the extension ring test comprise means for:

a. generating a random number 'n';

b. checking if the random number 'n' is an exact power of another positive integer;

if the random number 'n' is an exact power of another positive integer, then:

c. declaring the random number 'n' to be composite; and

if the random number 'n' is not an exact power of another positive integer, then:

d. performing an extension ring test, the extension ring test comprising means for:

i. determining the smallest number 'r' less than the random number 'n', the number 'r' satisfying the following conditions:

1. the number 'r' is a prime number;
2. the largest prime factor 'q' of (r – 1) is greater than or equal to $(4\sqrt{r} \log_2 n)$;
3. $n^{(r-1)/q} \neq 1 \bmod (r)$; and

4. the greatest common divisor of the number 'r' and the random number 'n' is equal to 1;

if no number 'r' satisfying all the conditions specified in step a exists, then for all values of the number 'r' less than the random number 'n':

ii. performing a check whether the greatest common divisor of the number 'r' and the random number 'n' is greater than 1; and

if the greatest common divisor of 'r' and 'n' is greater than 1 for any value of the number 'r', then:

1. means for declaring the number 'n' to be composite; and

if the greatest common divisor of 'r' and 'n' is equal to 1 for all values of the number 'r', then:

2. means for declaring the number 'n' to be prime;

if a number 'r' satisfying the conditions specified in step a exists, then:

iii. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and $(2\sqrt{r} \log_2 n)$, then:

1. means for declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$, then:

2. means for declaring the random number 'n' to be prime.